Dialog eLink: Order File History
21/3,K/2 (Item 1 from file: 350)
DIALOG(R)File 350: Derwent WPIX

0016919605
WPI Acc no: 2007-634671/200760
Related WPI Acc No: 2003-288827; 2007-558296; 2007-558297
XRPX Acc No: N2007-495039

Block cipher device for encrypting and decrypting digital data in cryptographically secured digital communication system, combines two key data sub blocks derived from contents of shift registers into single key data sub blocks

Patent Assignee: HARRIS CORP (HARO)
Inventor: KURDZIEL M T

Patent Family (1 patents, 1 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	Type
US 20070116272	A1	20070524	US 2001893461	A	20010629	200760	B
			US 2006498038	A	20060803		

Priority Applications (no., kind, date): US 2001893461 A 20010629; US 2006498038 A 20060803

Patent Details

Patent Number	Kind	Lan	Pgs	Draw	Filing Notes	
US 20070116272	A1	EN	12	6	Division of application	US 2001893461

Block cipher device for encrypting and decrypting digital data in cryptographically secured digital communication system, combines two key data sub blocks derived from contents of shift registers into single key data sub blocks Alerting Abstract
...NOVELTY - The **key** schedulers randomize a **portion** of **key** data **block** using the respective **shift** registers. The two modulo summing combiner serially combines a serial output from the shift register and the serial output from the key schedulers so as to provide two **combined** data outputs. Another modulo summing **combiner combines** two key **data sub** blocks derived from the contents of the **shift** registers into a single **key data sub** blocks so as to provide key **data sub** blocks to different encryption stages. ...ADVANTAGE - The security against available cryptanalysis or cracking techniques is enhanced **while** maintaining the compatibility. The cryptographic strength is increased without proportional increase in gate count of... ...DESCRIPTION OF DRAWINGS - The figure shows a block diagram of the **block cipher** device. Original Publication Data by AuthorityArgentina**Publication No. Claims:1-7**. (canceled)**8**. In a **block cipher** device used in encrypting and decrypting information in a cryptographically secured

digital communication system having plural encryption stages that are computationally a function of an input **data** block, a control **data** block, a key **data sub**-block, and a key scheduler for randomizing the key **data sub**-block, the improvement wherein the **key** scheduler comprises:a first **shift** register;a first means for randomizing a **portion** of the **key** data **block** using said first **shift** register;a first modulo two summing combiner for serially combining a serial output from the... ... shift register and the serial output from said first randomizing means to provide a first **combined data** output;a first key **data sub**-block derived from the contents of said first shift register;a second shift register;a second means for randomizing a **portion** of the **key** data **block** using said second **shift** register;a second modulo two summing combiner for serially combining the serial output from the... ... shift register and the serial output from said second randomizing means to provide a second **combined data** output;a second key **data sub**-block derived from the contents of the second shift register;a third modulo two summing **combiner** for **combining** said first key **data sub**-block and said second key **data sub**-block to produce a third key **data sub**-block;a first function unit that is computationally a function of the second key **data sub**-block for providing a fourth key **data sub**-block; andcircuit means for providing said first, third and fourth key **data sub**-blocks to different ones of said plural encryption stages.Basic Derwent Week: 200760

Dialog eLink: Order File History
21/3,K/16 (Item 15 from file: 350)
DIALOG(R)File 350: Derwent WPIX

0009322938
WPI Acc no: 1999-254491/**199921**
Related WPI Acc No: 2001-482049; 2001-512821; 2002-061520
XRPX Acc No: N1999-189449
N-bit block of data encrypting
Patent Assignee: LUYSTER F C (LUYS-I)
Inventor: LUYSTER F C

Patent Family (11 patents, 79 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	Type
WO 1999014889	A1	19990325	WO 1998US19255	A	19980916	199921	B
AU 199895690	A	19990405	AU 199895690	A	19980916	199933	E
EP 1016240	A1	20000705	EP 1998949350	A	19980916	200035	E
			WO 1998US19255	A	19980916		
US 6199162	B1	20010306	US 199759142	P	19970917	200152	E
			US 199762992	P	19971023		
			US 199764331	P	19971030		
			US 199894632	P	19980730		
			US 199896788	P	19980817		
			US 199896921	P	19980818		
			US 199898905	P	19980902		
			US 1998154391	A	19980916		
			US 2000506285	A	20000217		
US 6182216	B1	20010130	US 199759142	P	19970917	200156	E
			US 199762992	P	19971023		
			US 199764331	P	19971030		
			US 199894632	P	19980730		
			US 199896788	P	19980817		
			US 199896921	P	19980818		
			US 199898905	P	19980902		
			US 1998154391	A	19980916		
US 20010038693	A1	20011108	US 199759142	P	19970917	200208	E

			US 199762992	P	19971023		
			US 199764331	P	19971030		
			US 199894632	P	19980730		
			US 199896788	P	19980817		
			US 199896921	P	19980818		
			US 199898905	P	19980902		
			US 1998154391	A	19980916		
			US 2000506285	A	20000217		
			US 2000725596	A	20001129		
US 20020118827	A1	20020829	US 199759142	P	19970917	200259	E
			US 199762992	P	19971023		
			US 199764331	P	19971030		
			US 199894632	P	19980730		
			US 199896788	P	19980817		
			US 199896921	P	19980818		
			US 199898905	P	19980902		
			US 1998154391	A	19980916		
			US 2000506285	A	20000217		
			US 2000725596	A	20001129		
			US 20013503	A	20011023		
US 6578150	B2	20030610	US 199759142	P	19970917	200340	E
			US 199762992	P	19971023		
			US 199764331	P	19971030		
			US 199894632	P	19980730		
			US 199896788	P	19980817		
			US 199896921	P	19980818		
			US 199898905	P	19980902		
			US 1998154391	A	19980916		
			US 2000506285	A	20000217		
			US 2000725596	A	20001129		
US 6182216	C1	20030708	US 199759142	P	19970917	200347	E
			US 199762992	P	19971023		
			US 199764331	P	19971030		
			US 199894632	P	19980730		
			US 199896788	P	19980817		

			US 199896921	P	19980818		
			US 1998154391	A	19980916		
US 6199162	C1	20040525	US 199759142	P	19970917	200436	E
			US 199762992	P	19971023		
			US 199764331	P	19971030		
			US 199894632	P	19980730		
			US 199896788	P	19980817		
			US 1998154391	A	19980916		
			US 2000506285	A	20000217		
US 6751319	B2	20040615	US 199759142	P	19970917	200439	E
			US 199762992	P	19971023		
			US 199764331	P	19971030		
			US 199894632	P	19980730		
			US 199896788	P	19980817		
			US 199896921	P	19980818		
			US 199898905	P	19980902		
			US 1998154391	A	19980916		
			US 2000506285	A	20000217		
			US 2000725596	A	20001129		
			US 20013503	A	20011023		

Priority Applications (no., kind, date): US 199759142 P 19970917; US 199762992 P 19971023; US 199764331 P 19971030; US 199894632 P 19980730; US 199896788 P 19980817; US 199896921 P 19980818; US 199898905 P 19980902; US 1998154391 A 19980916; WO 1998US19255 A 19980916; US 2000506285 A 20000217; US 2000725596 A 20001129; US 20013503 A 20011023

Patent Details

Patent Number	**Kind**	**Lan**	**Pgs**	**Draw**	**Filing Notes**	
WO 1999014889	A1	EN	131	14		
National Designated States,Original	AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GE GH HU IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG UZ VN YU ZW					
Regional Designated States,Original	AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW NL OA PT SD SE SZ UG ZW					
AU 199895690	A	EN			Based on OPI patent	WO 1999014889

EP 1016240	A1	EN			PCT Application	WO 1998US19255
					Based on OPI patent	WO 1999014889
Regional Designated States,Original	AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE					
US 6199162	B1	EN	57		Related to Provisional	US 199759142
					Related to Provisional	US 199762992
					Related to Provisional	US 199764331
					Related to Provisional	US 199894632
					Related to Provisional	US 199896788
					Related to Provisional	US 199896921
					Related to Provisional	US 199898905
					Continuation of application	US 1998154391
US 6182216	B1	EN	47		Related to Provisional	US 199759142
					Related to Provisional	US 199762992
					Related to Provisional	US 199764331
					Related to Provisional	US 199894632
					Related to Provisional	US 199896788
					Related to Provisional	US 199896921
					Related to Provisional	US 199898905
US 20010038693	A1	EN	49		Related to Provisional	US 199759142
					Related to Provisional	US 199762992
					Related to Provisional	US 199764331
					Related to Provisional	US 199894632
					Related to Provisional	US 199896788
					Related to Provisional	US 199896921
					Related to Provisional	US 199898905
					Continuation of application	US 1998154391
					Continuation of application	US 2000506285
					Continuation of patent	US 6182216
					Continuation of patent	US 6199162
US 20020118827	A1	EN			Related to Provisional	US 199759142
					Related to Provisional	US 199762992
					Related to Provisional	US 199764331

					Related to Provisional	US 199894632
					Related to Provisional	US 199896788
					Related to Provisional	US 199896921
					Related to Provisional	US 199898905
					Continuation of application	US 1998154391
					Continuation of application	US 2000506285
					Continuation of application	US 2000725596
					Continuation of patent	US 6182216
					Continuation of patent	US 6199162
US 6578150	B2	EN			Related to Provisional	US 199759142
					Related to Provisional	US 199762992
					Related to Provisional	US 199764331
					Related to Provisional	US 199894632
					Related to Provisional	US 199896788
					Related to Provisional	US 199896921
					Related to Provisional	US 199898905
					Continuation of application	US 1998154391
					Continuation of application	US 2000506285
					Continuation of patent	US 6182216
					Continuation of patent	US 6199162
US 6182216	C1	EN			Related to Provisional	US 199759142
					Related to Provisional	US 199762992
					Related to Provisional	US 199764331
					Related to Provisional	US 199894632
					Related to Provisional	US 199896788
					Related to Provisional	US 199896921
US 6199162	C1	EN			Related to Provisional	US 199759142
					Related to Provisional	US 199762992
					Related to Provisional	US 199764331
					Related to Provisional	US 199894632
					Related to Provisional	US 199896788
					Continuation of application	US 1998154391
					Continuation of patent	US 6182216
US 6751319	B2	EN			Related to Provisional	US 199759142
					Related to Provisional	US 199762992

					Related to Provisional	US 199764331
					Related to Provisional	US 199894632
					Related to Provisional	US 199896788
					Related to Provisional	US 199896921
					Related to Provisional	US 199898905
					Continuation of application	US 1998154391
					Continuation of application	US 2000506285
					Continuation of application	US 2000725596
					Continuation of patent	US 6182216
					Continuation of patent	US 6199162
					Continuation of patent	US 6578150

...**Original Titles:**IMPROVED **BLOCK CIPHER** METHOD... ...**Block cipher** method... ...**Block cipher** method... ...**Block cipher** method... ...**Block cipher** method... ...**Block cipher** method... ...**Block cipher** method... ...IMPROVED **BLOCK CIPHER** METHOD **Alerting Abstract** ...NOVELTY - The method involves first bit-**moving** variable bits of a round **segment** of data derived from one of the first and second round segments of data by set numbers of bits where most of the resulting bits affect the n-bit **block** of data. The first bit-**moving** is an operation selected from a group consisting of circular bit-rotation by nonzero numbers... ... Linearly combine (block (132) using the operator L5) that intermediate segment and Ri producing a **replacement value** of Ri. Then, extract (block (134) a value V from R0) by taking f of the lsb bits of register (R0). Rotate (block (136) the **replacement value** of RI by the **value** V just extracted. This resulting value of R1 after the rotation is the new value... ... a binary **block cipher** data transformation **system a** method of key expansion for **block ciphers** ... ... USE - The invention relates to **block cipher** secret-key cryptographic systems and methods.... ... key expansion, particularly for data-dependent encryption, which decreases the time required to prepare a **block cipher** to encrypt or decrypt digital packets **of bytes**. The cryptographic system and method use minimal numbers of s-boxes with a novel iterative calculation where the **block cipher** does not require an excessive startup **time**, **yet** is simple, secure and efficient for bulk encryption **while** uses no more on-chip cache than **necessary**. The invention provides a novel mechanism and method for complex key expansion, which uses a minimum amount of time to prepare a **block cipher** to encrypt or decrypt a large **file and** which nevertheless ensures that the sub-keys generated by the method reflect every **bit** of the key in a complex uncorrelated mannerOriginal Publication Data by AuthorityArgentina**Publication No.** ...**Original Abstracts:**includes a computing unit for the execution of each round; memory for storing and loading **segments**; a bit-**moving** function capable of rotating, shifting, **or** bit-permute round segments by predetermined numbers **of** bits **preferably** to achieve **active** and effective **fixed** rotation; **a** linear **combination** function which provides new one-to-one round segments using a round operator generally from... ... unit for the execution of each round; memory for storing and loading segments; a bit-**moving** function capable of rotating, **shifting**, or bit-permute round **segments by** predetermined numbers **of bits** preferably to achieve **active** and **effective** fixed rotation; **a** linear **combination function** which **provides** new one-to-one round segments using a round operator generally from one algebraic group... ... includes a computing unit for the execution of each round; memory for storing and loading **segments**; a bit-**moving** function capable of rotating, shifting, or bit-permute round **segments** by **predetermined** numbers of **bits** preferably to achieve active **and** effective **fixed** rotation; a **linear combination** function **which** provides **new** one-to-one round segments using a round operator generally from one algebraic group to... includes a computing unit for the execution of each round; memory for storing and loading **segments**; a bit-**moving** function capable of rotating, shifting, or bit-permute round **segments** by **predetermined** numbers of **bits** preferably to achieve active **and** effective **fixed** rotation; a **linear combination** function **which** provides **new** one-to-one round segments using a round operator generally from one algebraic group to... ... includes a computing unit for the execution of each round; memory for storing and loading **segments**; a bit-**moving** function capable of rotating, **shifting**, or bit-permute round **segments** by predetermined numbers of bits **preferably** to achieve **active** and effective fixed rotation; **a** linear **combination** function which **provides** new one-**to**-one round segments using a round operator generally from one algebraic group to combine two... ... includes a computing unit for the execution of each round; memory for storing and loading **segments**; a bit-**moving** function capable of rotating, **shifting**, or bit-permute round **segments** by predetermined numbers of bits preferably to achieve active and **effective** fixed **rotation**; **a** linear combination function which **provides** new **one**-to-one **round segments** using a round operator generally from one algebraic group to combine two different one-to... ... for storing and loading segments by predetermined numbers of bits preferably to achieve active and **effective** fixed rotation; a linear **combination** function (132) which provides new one-to-one round segments using a round operator generally **from** one **algebraic** group to **combine** two different one-to-one round segments taken from one-to-one round segment set;... ...**Claims:**enciphered plaintext originating from plaintext which has been enciphered by enciphering said plaintext in a **block cipher**, said enciphering using a secret key, said **enciphering comprising**:processing round segments in a plurality of rounds of said **block cipher**, said plurality of rounds including a plurality of bit-**moving rounds**, each of said bit-**moving** rounds transforming input primary **segments** having a total of n **bits** of data into output **primary segments** having a total of n bits of data, each of said input primary segments originating directly or indirectly from said plaintext, each of said **round segments** of each said bit-**moving** round comprising a **segment** which **originates** from at least one **of** said input primary **segments** of said bit-**moving** round, each output primary **segment** of **each** said bit-**moving round** being equal to one **of** said round **segments** of said bit-**moving** round, said processing round **segments** in each of said bit-**moving** rounds comprising,predetermined bit-**moving** at least one present bit-**value** in a present bit-position of **one** of said round **segments** of said bit-**moving** round to determine a bit-value in an other bit-position of **one** of said round **segments** of said bit-**moving** round, said present bit-position being different than **said** other bit-position,**variable** bit-**moving** bits of one of said round **segments** of said bit-**moving** round by a number of bits dependent on a value from data of one **of** said round **segments** of said bit-**moving** round, andwherein each of said segments is an ordered **set** of bits.... ... What is claimed is:**1**. A method of enciphering plaintext in a **block cipher**, comprising:processing round segments in a plurality of rounds of said **block cipher**, said processing round segments in each of said rounds comprising,predetermined bit-**moving** at least **one present** bit-value in a present bit-position of one of said round segments **of said** round to determine a bit-value in an other bit-position of one of **said** round **segments** of said round, andvariable bit-moving bits of one of said round segments of... ... data; andencrypting the n-bit block of data using a secret key and a **block cipher** comprising:performing a plurality of encrypting rounds on said first and second round segments of data, at least five of said encrypting rounds comprising,modifying said first **round** segment of **data** with **values** from **the** first linear **combining** of first, second, and third variable **segments**, **said** first variable segment of at least 64 bits comprising at least 50 variable bits derived... ... from said first round segment of data, said second variable segment of at least 64 **bits** comprising at **least** 50 **variable bits** from a first **derivation** from said second round segment of data, and said third variable segment comprising a value... ... selected from a lookup table in response to at least a portion of the n-**bit** block of **data**, where said **first** linear **combining** is selected from a group consisting of either **direct** linear combination, indirect linear **combination**, andfirst bit-**moving** variable **bits** of a round **segment** of data derived from one of said first and second round segments of data by predetermined **numbers of bits** where **most** of the resulting **bits affect** the n-**bit** block of **data**, and where first **bit**-moving is an **operation** selected from a group **consisting** of circular bit-rotation by non-**zero** numbers of bits, logical bit-**shift** by non-zero numbers of **bits**, non-identity bit-permutation... ... A method of enciphering plaintext in a **block cipher**, said enciphering using a secret key, said method comprising:processing round segments in a plurality of rounds of said **block cipher**, said plurality of rounds including a plurality of bit-moving rounds, each of said bit-**moving** rounds transforming input primary **segments** having a total of n bits of data into out-put primary segments having **a total** of n bits of data, each of said input primary segments originating directly or indirectly from said plaintext, each of said **round segments** of each said bit-**moving** round comprising a segment **which** originates from at least one **of** said input primary **segments of** said bit-**moving** round, each output primary **segment** of each said bit-**moving** round being equal to one of said round **segments** of said bit-**moving round**, said processing round **segments** in each of said bit-**moving** rounds **comprising**,predetermined bit-**moving** at **least** one present bit-**value** in a present bit-position of one of said round segments of said bit-**moving** round to determine a **bit**-value in an other **bit**-position of one of said round **segments** of **said** bit-moving round, **said** present bit-position being **different** than said other bit-position,**variable** bit-**moving** bits of one of **said** round **segments** of said bit-**moving** round by a number of bits dependent on a value from data of one **of** said round **segments** of said bit-**moving** round, andwherein each of said segments is an **ordered** set of bits.**What** is claimed is:1. A data signal propagated over a propagation medium, said data signal... ... enciphered plaintext originating from plaintext which has been enciphered by enciphering said plaintext in a **block cipher**, said enciphering using a secret key, said enciphering comprising:processing round segments in a plurality of rounds of said **block cipher**, said plurality of rounds including a plurality of bit-moving rounds, each of said bit-**moving** rounds transforming input primary **segments** having a total of n bits of data into output primary segments having a total... ... of data, each of said input primary segments originating directly or indirectly from said plaintext, **each of** said round **segments** of each **said** bit-**moving** round comprising a **segment** which **originates** from at least one of said input **primary segments** of said bit-**moving** round, each output primary **segment of** each said bit-**moving** round **being** equal to one of **said** round segments of said bit-**moving** round, said processing round **segments in** each of said bit-**moving** rounds comprising,predetermined bit-**moving** at least one **present** bit-value in a present bit-position of one of said **round segments** of said bit-**moving** round to determine **a** bit-value in an other bit-position of one of said round segments of **said** bit-**moving** round, said **present** bit-position being different **than** said other bit-position,variable bit-**moving** bits of one of said **round** segments of said bit-**moving** round by a number of **bits** dependent on a value from data **of** one of said round **segments** of said bit **moving** round, andwherein each of said **segments is** an ordered set **of** bits.What is claimed is:1. A method of using a secret key to encipher or **decipher** n-bit data **having** a plurality of words, comprising:variably rotating bits originating from one of said words **to replace** at least one **value** of any of said words with at least one other value, said variably rotating being... ... of said words;fixedly rotating bits of any of said words having at least 32 **bits** to **replace** at least one **value** of any of said words with at least one other value, said fixedly rotating being... ... circumflex over ( )}f=n/x with n being the number of bits of said n-**bit data** and x being the **number** of words **of** said plurality of **words**; andrepeating said variably rotating and said moving for a number of rounds, said numberBasic Derwent Week: **199921**

Dialog eLink: Order File History
21/3,K/17 (Item 16 from file: 350)
DIALOG(R)File 350: Derwent WPIX

0009151425
WPI Acc no: 1999-073436/**199907**
XRPX Acc No: N1999-053875

Block cipher secure against differential and linear cryptanalysis - divides the input into two half-blocks which are combined with the key octet by octet, then shifted left after passing through substitution boxes

Patent Assignee: SAMSUNG ELECTRONICS CO LTD (SMSU)
Inventor: CHA Y; CHA Y T; LEE C; LEE C H

Patent Family (10 patents, 6 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	Type
FR 2765056	A1	19981224	FR 19987753	A	19980619	199907	B
GB 2327581	A	19990127	GB 199811900	A	19980604	199907	E
DE 19827904	A1	19990114	DE 19827904	A	19980623	199908	E
JP 11073101	A	19990316	JP 1998175844	A	19980623	199921	E
GB 2327581	B	19990804	GB 199811900	A	19980604	199933	E
KR 1999002840	A	19990115	KR 199726558	A	19970623	200011	E
DE 19827904	C2	20000511	DE 19827904	A	19980623	200028	E
JP 3148181	B2	20010319	JP 1998175844	A	19980623	200125	E
US 6314186	B1	20011106	US 199895845	A	19980611	200170	E
KR 389902	B	20030922	KR 199726558	A	19970623	200416	E

Priority Applications (no., kind, date): KR 199726558 A 19970623

Patent Details

Patent Number	Kind	Lan	Pgs	Draw	Filing Notes	
FR 2765056	A1	FR	20	3		
JP 11073101	A	JA	8			
KR 1999002840	A	KO		3		
JP 3148181	B2	JA	11		Previously issued patent	JP 11073101
KR 389902	B	KO			Previously issued patent	KR 99002840

Block cipher secure against differential and linear cryptanalysis... ...divides the

input into two half-blocks which are combined with the key octet by octet, then shifted left after passing through substitution boxes ...**Original Titles:Block cipher** algorithm having a robust security against differential cryptanalysis, linear cryptanalysis and higher-order differential cryptanalysis. **Alerting Abstract** ...left, and the results used to form a new second half of the input block, **while** the old second half forms a new half... Original Publication Data by AuthorityArgentina**Publication No. Original Abstracts:**The present invention relates to the **block cipher** algorithm based on the prior Feistel type **block cipher** algorithm (or similar to DES algorithm). Usually the security of Feistel type **block cipher** algorithm depends on the structure of its round function. More specifically, the present invention relates to the round function structure of the Feistel type **block cipher** algorithm, in the instance that the round input data block is divided into 8-**bit** blocks and the divided **sub**-blocks are fed, with the **combined** output **data** of the previous S-box, into 256x8 S-box, except for the first input **sub-data** block. The first **sub-data** block one is directly fed into the first S-box. The total output data block... ...**Claims:**A **block cipher** method having a round process and having a key scheduling algorithm, comprising: (a) dividing a... ... OR operation with the second half block and an N-byte round key; (c) dividing **a result** of step (b) into N divided blocks, sending a first divided block to a first... Basic Derwent Week: **199907**

Dialog eLink: Order File History
21/3,K/27 (Item 26 from file: 350)
DIALOG(R)File 350: Derwent WPIX

0001166172
WPI Acc no: 1976-F1156X/**197622**
Block cipher system for data security - with result of one product block cipher iteration serving as argument of next iteration
Patent Assignee: IBM CORP (IBMC)
Inventor: EHRSAM W F; MEYER C H W; POWERS R L; PRENTICE P N; SMITH J L; TUCHMAN W L

Patent Family (7 patents, 6 countries)

Patent Number	**Kind**	**Date**	**Application Number**	**Kind**	**Date**	**Update**	**Type**
US 3958081	A	19760518	US 1975552685	A	19750224	197622	B
DE 2558206	A	19760909	DE 2558206	A	19751223	197638	E
FR 2301873	A	19761022				197652	E
DE 2558206	B	19770421	DE 2558206	A	19751223	197717	E
GB 1480859	A	19770727				197730	E
CA 1048935	A	19790220				197910	E
IT 1055306	B	19811221				198211	E

Priority Applications (no., kind, date): US 1975552685 A 19750224

Patent Details

Patent Number	**Kind**	**Lan**	**Pgs**	**Draw**	**Filing Notes**
CA 1048935	A	EN			

Block cipher system for data security... ...with result of one product block cipher iteration serving as argument of next iteration ...**Original Titles:Block cipher** system for data security **Alerting Abstract** ...data bits. The data bits of the expanded message block are combined by modulo-2 **addition** with an equal **number** of cipher key bits, selected in accordance with an arbitrary but fixed permutation, to produce ... ...different nonlinear substitution function boxes. The substitution boxes perform nonlinear transformation functions to produce a **substitution** set of **bits** which are equal in number to the number of data bits in the first half... Original Publication Data by AuthorityArgentina**Publication No.** ...**Original Abstracts:**data bits. The data bits of the expanded message block are combined by modulo-2 **addition** with an equal **number** of cipher key bits, selected in accordance with an arbitrary but fixed permutation, to

produce... ... function boxes. The substitution boxes perform a plurality of nonlinear transformation functions to produce a **substitution** set of **bits** which are equal in number to the number of data bits in the first half of the message block. The **substitution** set of **bits** is then subjected to a linear transformation in accordance with an arbitrary but fixed permutation. The combined nonlinear transformation and linear transformation results in a product **block cipher** of the first half of the message block. The second half of the message block is then modified by modulo-2 addition with the product **block cipher** of the first half of the message block to produce a modified second half of... ... the message block then replaces the first half of the message block which at the **same time** replaces the second half of the message block in preparation for the next iteration operation. **During** the next iteration operation, the cipher **key** bits are **shifted** according to a predetermined shift schedule to provide a new set of permuted cipher key... ... then used with the new set of permuted cipher ket bits in a similar product **block cipher** operation, the result of which is used to modify the first half of the message... ... message block then replaces the modified second half of the message block which at the **same time** replaces the first half of the message block in preparation for the next iteration operation. **During** each of the remaining iteration operations of the enciphering process except the last, the cipher **key** bits are **shifted** according to the predetermined shift schedule, a modified half of the message block is remodified according to a product **block cipher** of the previously modified half of the message block and the resulting remodified half of a message block is effectively transposed with the previously modified half of the message block. **During** the last iteration operation, the cipher **key** bits are **shifted** a last time according to the shift schedule and a last remodification of a modified half of the message block is performed according to a product **block cipher** of the previously modified half of the message block but the resulting remodified half of... ... carried out by the same series of iteration operations under control of the same cipher **key shifted during** the iteration operations according to a predetermined shift schedule in a direction opposite to that...
Basic Derwent Week: **197622**

Dialog eLink: Order File History
29/3,K/7 (Item 6 from file: 350)
DIALOG(R)File 350: Derwent WPIX

0013532453 *Drawing available*
WPI Acc no: 2003-625890/**200359**
Related WPI Acc No: 2004-756568; 2008-B59223
XRPX Acc No: N2003-498006
Byte substitution operation performing apparatus for encryption and decryption of advanced encryption standard, has multiplexer to receive look-up table data code based on output of primary multiplexer and matrix operation module
Patent Assignee: IND TECHNOLOGY RES INST (INTE-N); LU C (LUCC-I); TSENG S (TSEN-I)
Inventor: LIU J; LU C; TSENG S; TZENG S

Patent Family (4 patents, 3 countries)

Patent Number	**Kind**	**Date**	**Application Number**	**Kind**	**Date**	**Update**	**Type**
US 20030099352	A1	20030529	US 2002108355	A	20020329	200359	B
GB 2383860	A	20030709	GB 200222149	A	20020924	200359	E
TW 527783	A	20030411	TW 2001124577	A	20011004	200366	E
US 7236593	B2	20070626	US 2002108355	A	20020329	200742	E

Priority Applications (no., kind, date): TW 2001124577 A 20011004; US 2002108355 A 20020329

Patent Details

Patent Number	**Kind**	**Lan**	**Pgs**	**Draw**	**Filing Notes**
US 20030099352	A1	EN	18	9	
TW 527783	A	ZH			

Byte substitution operation performing apparatus for encryption and decryption of advanced encryption standard, has multiplexer to receive look-up table data code based on output of primary multiplexer... Original Titles: Apparatus for encryption and decryption, capable of use in encryption and decryption of **advanced encryption standard** ... ...Apparatus for encryption and decryption, capable of use in encryption and decryption of **advanced encryption standard Alerting Abstract** ... apparatus for performing **column mixing** operation; apparatus for performing **key** expansion operation; and apparatus for encryption and decryption... ... USE - For encryption and decryption of **advanced encryption standard** (**AES**).Original Publication Data by AuthorityArgentina**Publication No. Original Abstracts:**An apparatus for encryption and

decryption, capable of use in encryption and decryption of **advanced encryption standard**. **Byte** substitution operation and inverse **byte** substitution operation are to be **combined**. **Byte** substitution operation can be expressed as y=M*multiplicative... ... inverse(x)+c **while** inverse byte substitution operation can be expressed as x=multiplicative... ... inverse(x), the lookup tables for use in byte substitution and inverse **byte** substitution operations are to be **combined** according to the invention so as to lower hardware complexity of the implementation. In addition, main operations of **column mixing** operation and inverse **column mixing** operation are to be rearranged to combine the two operations in part, resulting in simplified... ... An apparatus for encryption and decryption, capable of use in encryption and decryption of **advanced encryption standard**. **Byte** substitution operation and inverse **byte** substitution operation are to be **combined**. **Byte** substitution operation can be expressed as y=M*multiplicative... ... inverse(x)+c **while** inverse byte substitution operation can be expressed as x=multiplicative... ... inverse(x), the lookup tables for use in byte substitution and inverse **byte** substitution operations are to be **combined** according to the invention so as to lower hardware complexity of the implementation. In addition, main operations of **column mixing** operation and inverse **column mixing** operation are to be rearranged to combine the two operations in part, resulting in simplified... ...**Claims:**to output a required output data code, capable of use in encryption and decryption of **advanced encryption standard** (**AES**), the apparatus comprising:an inverse matrix operation module for receiving the input data code so... ... to output a required output data code, capable of use in encryption and decryption of **advanced encryption standard** (**AES**), the apparatus comprising: an inverse matrix operation module for receiving the input data code so...
Basic Derwent Week: **200359**

Dialog eLink: Order File History
29/3,K/19 (Item 18 from file: 350)
DIALOG(R)File 350: Derwent WPIX

0009261820 *Drawing available*
WPI Acc no: 1999-190071/**199916**
XRPX Acc No: N1999-139045

Operating method for processor in data encryption e.g. key insertion, message authentication

Patent Assignee: STIEBEL J (STIE-I)
Inventor: STIEBEL J

Patent Family (3 patents, 81 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	Type
WO 1999008411	A2	19990218	WO 1998IL369	A	19980806	199916	B
AU 199886440	A	19990301	AU 199886440	A	19980806	199928	E
EP 1062755	A2	20001227	EP 1998937742	A	19980806	200102	E
			WO 1998IL369	A	19980806		

Priority Applications (no., kind, date): IL 121499 A 19970808; IL 121500 A 19970808; IL 124705 A 19980601

Patent Details

Patent Number	Kind	Lan	Pgs	Draw	Filing Notes	
WO 1999008411	A2	EN	151	36		
National Designated States,Original	AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GE GH GM HR HU ID IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG US UZ VN YU ZW					
Regional Designated States,Original	AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW NL OA PT SD SE SZ UG ZW					
AU 199886440	A	EN			Based on OPI patent	WO 1999008411
EP 1062755	A2	EN			PCT Application	WO 1998IL369
					Based on OPI patent	WO 1999008411
Regional Designated States,Original	AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE					

Operating method for processor in data encryption e.g. key insertion, message authentication Alerting Abstract ...distinct single size portion of the result is folded in several companion executions. Thus, every **simultaneous** encryption depends in all bits of input into an s-box on every other **parallel** encryption. The folding is performed so that the inputs to the s-box depend on... ...USE - Processor in **data** encryption e.g. key **insertion**, message authentication... Original Publication Data by AuthorityArgentina**Publication No.** ...**Original Abstracts:**exclusive-or is replaced within the F function with a form of multiplication. Thus, every **simultaneous** encryption depends in **all** of the bits of input into the s-box on every other **parallel** encryption. Any invertable **group** operation could be used in place of multiplication. The principle requirement is that every input... ... the present invention. The recommended key schedule for Feistel and other blocks ciphers uses the **block cipher** to cause **complete mixing** of the **key bits** and pseudo-**random** expansion into conveniently sized subkeys. A subkey chaining mode for influencing future encryptions of **block ciphers** in place **of cipher** block chaining mode is proposed. A Feistel structure allowing for further extension of block length... ... exclusive-or is replaced within the F function with a form of multiplication. Thus, every **simultaneous** encryption depends in all of the bits of **input** into the s-box on every other **parallel** encryption. Any invertable group operation could be used **in** place of multiplication. The principle requirement is that every input bit will influence every output... ... of the method of the present invention. The recommended key schedule for Feistel and other **blocks** ciphers uses the **block cipher** to cause complete **mixing** of the **key bits and** pseudo-random expansion **into** conveniently sized **subkeys**. A **subkey** chaining mode for influencing future encryptions of **block ciphers** in place of cipher block chaining mode **is proposed**. A Feistel structure allowing for further extension of block length for subkey chaining output is... ... Basic Derwent Week: **199916**...

Dialog eLink: Order File History
9/3K/3 (Item 3 from file: 349)
DIALOG(R)File 349: PCT FULLTEXT

00989343

APPARATUS AND METHOD FOR PERFORMING A CRYPTOGRAPHIC ALGORITHM
APPAREIL ET PROCEDE D'EXECUTION D'UN ALGORITHME CRYPTOGRAPHIQUE

Patent Applicant/Patent Assignee:

- **INFINEON TECHNOLOGIES AG**; St.-Martin-Str. 53, 81669 Munchen
  DE; DE(Residence); DE(Nationality)
  (For all designated states except: US)
- **VALVERDE Antonio**; Unterhachinger Str. 33 a, 81737 Munchen
  DE; DE(Residence); ES(Nationality)
  (Designated only for: US)
- **SEIFERT Jean-Pierre**; Harsdorferstr. 1, 81669 Munchen
  DE; DE(Residence); DE(Nationality)
  (Designated only for: US)

Patent Applicant/Inventor:

- **VALVERDE Antonio**
  Unterhachinger Str. 33 a, 81737 Munchen; DE; DE(Residence); ES(Nationality);
  (Designated only for: US)
- **SEIFERT Jean-Pierre**
  Harsdorferstr. 1, 81669 Munchen; DE; DE(Residence); DE(Nationality);
  (Designated only for: US)

Legal Representative:

- **SCHOPPE Fritz(et al)(agent)**
  Schoppe, Zimmermann, Stockeler & Zinkler, Postfach 71 08 67, 81458 Munchen; DE;

	Country	Number	Kind	Date
Patent	WO	200319357	A1	<B>20030306</B>
Application	WO	2001EP9583		20010820
Priorities	WO	2001EP9583		20010820

Designated States: (All protection types applied unless otherwise stated - for applications 2004+)

[EP] AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LU; MC; NL; PT; SE; TR;

[OA] BF; BJ; CF; CG; CI; CM; GA; GN; GQ; GW; ML; MR; NE; SN; TD; TG;

[AP] GH; GM; KE; LS; MW; MZ; SD; SL; SZ; TZ; UG; ZW;

[EA] AM; AZ; BY; KG; KZ; MD; RU; TJ; TM;

Language Publication Language:	English
Filing Language:	English
Fulltext word count:	8257

English Abstract:

...a CPU (12) and a coprocessor (14). One step of the cryptographic algorithm is a **mix columns** transformation on **mix columns** input data. The CPU (12) is arranged for providing the **mix columns** input data. The coprocessor (14) is arranged for performing at least a part of the **mix columns** transformation on the **mix columns** transformation with an arithmetic unit which conducts calculations for a number of data units in **parallel**, said number being equal to or greater than the number of data units of a column. By performing the **mix columns** transformation using CPU and a coprocessor having a long integer arithmetic unit, the execution time...

Detailed Description:

...Fig. 2. Before the first round starts, there has to be performed a so-called **add round key** operation, which is described later on. The original state array 302 (Fig. 3) is, therefore ...round 202 which consists of several consecutive transformations. These are the byte substitution 204, the **shift rows** operation 206, the mixed columns operation 208 and an **add round key** operation 210. For ease of illustration, also the data between blocks 204 to 210 are...is processed, a final AES round consists of a byte substitution operation followed by a **shift rows** operation which again is followed by a final **add round key** operation. The output of the final **add round key** operation are the output bytes 304 illustrated in Fig. 3.

The byte substitution operation shown each byte of the state using a substitution table which is

also called **S- box**. This **S-box**, which is invertible, is
constructed by composing two transformations, wherein the
first of the two... ...28). The other of the two
transformations is the affine (over GF(2)) transformation.

The **shift rows** transformation 206 is a transformation in which
the bytes in the last three rows of...lower positions in the row, i.e. lower values of c in a
given row, **while** the "lowest" bytes wrap around into the
"top" of the row, i.e. higher values...state (note that this state consists of the
array of bytes output by the preceding **shift rows**
transformation 206 in Fig. 2) are replaced by the following
S'ij. This is indicated...reason for considering the
columns as several polynomials over GF(28).

Fig. 5 illustrates the **mix columns** transformation to show that
from one column ...0 = 0. Consequently,, the subtraction of polynomials is
identical to the addition of polynomials.

The **add round key** transformation 210 (Fig. 2) serves to add a
round key to the state by a ...works
in a reverse order. The individual transformation used in the
inverse cyphers are inverse **shift rows**, inverse byte
substitution, inverse **mix columns** and **add round key**. These
individual transformations process the state and are performed
as described in the AES standard...even more. This is due to
the fact that the software implementation of the inverse **mix
columns** transformation for an 8-bit CPU is less efficient than
the **mix column** transformation used ...the present invention to provide an
improved concept for performing a cryptographic algorithm
having a **mix column** transformation which is appreciated by the
customers and, at the **same time**, less costly.

This object is achieved by an apparatus for performing a
cryptographic algorithm in...the finding that, although
the AES algorithm is specially defined for 8-bit CPUs. the **mix
columns** transformation is especially suited for being at least
partly performed by a coprocessor having an... ...unit
arranged for conducting calculations for a number of data
units, for example, bits in **parallel**, the number of data units
being equal to or greater than the number of data units of a
column of the **mix column** input data which are the state bytes
in case of the AES algorithm.

The long integer arithmetic unit included in the coprocessor
is used to perform the **mix column** transformation. The long
integer arithmetic unit included in the coprocessor can be

designed for calculating one data group, for example one byte, of the **mix columns** transformation output data, i.e., the state after the **mix column** transformation, in **parallel**, when it has registers and calculation units for processing a number of bit in **parallel**, the number of bits being equal to the number of bits in one column. Then, one data group of the **mix columns** output data can be calculated after the other which is a so-called serial-**parallel** or hybrid mode. Preferably, the long arithmetic unit is designed for processing a number of bits in **parallel** which is equal to the number of bits of the whole state. In this case, a fully **parallel** calculation of the **mix columns** transformation can be obtained. Both embodiments are made possible by interpreting the polynomials involved with the **mix columns** transformation that have coefficients in GF(28) as polynomials in the field GF(2 32...is suited for carrying out the calculations in GF(2 32)
or, when the whole **mix columns** transformation is performed in **parallel**, in GF(2 1213
Preferred embodiments of the present invention are explained in detail with...standardized in the
AES standard having coefficients in GF(28);
Fig. 4b illustrates how a **mix columns** operation can be described as a matrix multiplication;
Fig. 4c illustrates an expanded representation of... ...6a shows the Xtime operation on the state which is used
for performing a fully **parallel** calculation of the **mix columns** operation;
Fig. 6b illustrates a flow chart to perform the Xtime operation shown in Fig. 6a;
Fig. 7 illustrates a sequence of steps to perform a fully **parallel mix columns** transformation;
Fig. 8 shows a sequence of steps to perform a fully **parallel** inverse **mix columns** transformation;
Fig. 9a illustrates other Xtime operations which can be used for carrying out a fully **parallel** inverse **mix columns** transformation in accordance with another embodiment of the present invention;
Fig. 9b illustrates a sequence of steps for performing a fully **parallel** inverse **mix columns** transformation using Xtime operations shown in Fig. 9a;
Fig. 10 illustrates a sequence of steps to perform a fully **parallel** key expansion;
Fig. 11 shows a step how to perform fully **parallel add round key** operation; and
Fig. 12 illustrates the inventive apparatus arranged for performing the key expansion transformation in the

CPU and the **mix columns** transformation in the coprocessor, in accordance with another embodiment of the present invention.

Fig. I... ...to Fig. 2, the cryptographic algorithm includes a sequence of steps, one step including a **mix columns** transformation 208 (Fig. 2) on **mix columns** input data, i.e., with respect to Fig. 2, the state output data received after the **shift rows** step 206. The **mix columns** operations operates to obtain **mix columns** output data. The **mix columns** input data includes an array of data groups, e.g. bytes, the array having a...apparatus 10 further comprises a coprocessor 14 for performing at least a part of the **mix columns** transformation on the **mix columns** input data. The coprocessor 14 includes an arithmetic unit arranged for conducting calculations for a number of data units in **parallel**. The number of data units being equal to or 5 greater than the number of... ...encryption according to the AES algorithm, the arithmetic unit in the coprocessor is designed for **parallel** computation of at least 32 bits in **parallel** in order ...o,,, at a time. Preferably, however, the arithmetic unit is designed for performing the complete **mix columns** transformation in **parallel**. In this case, the arithmetic unit is arranged for performing calculations on a number of...the arithmetic unit is arranged for conducting calculations for a number of data units in **parallel**, the number of data units being equal or greater than the number of data units... ...a column, one line of the calculations shown in Fig. 4c is calculated substantially in **parallel** such that this embodiment can be regarded as a kind of hybrid concept, in which one data group of the **mix columns** output data is calculated in **parallel** and the data groups themselves are calculated one after the other. In contrast thereto, for... ...term to XOR the results to get slo,,@.

In accordance with the present invention, the **mix columns** transformation which multiplies a 4-byte variable polynomial by a constant polynomial r(x) modulo...of the coprocessor is arranged for conducting calculations for a number of data units in **parallel**, the number of data units being equal to the number of data units included in the **mix columns** input data. The second embodiment provides for a fully **parallel** implementation of the **mix columns** transformation.

Preferably, the Xtime(state) operation is used. The Xtime operation is defined in the... ...is performed inside the coprocessor on the, for example, 16 bytes of the state in

parallel with the formula shown in Fig. 6a. (state) indicates the **mix columns** input data, i.e. the data output by the **shift rows** transformation 206.

In Fig. 6a, the meanings of the symbols in the Xtime operation are...values
for d are possible for other key sizes. The + sign indicates addition modulo 2, **while** the AND sign (&) indicates the logical AND operation. Finally, the << or >> signs indicate left and coprocessor to calculate
the Xtime operation on the state, i.e. the **mix columns** input data. To this end, the coprocessor has two temporary registers Tmpl and Tmp2 as...Based on the Fig. 6a and Fig. 6b definition of the Xtime operation, the whole **mix columns** transformation is defined to operate on the 16 bytes of the state in **parallel**.

Referring to Fig. 7, a sequence of steps controlled by a sequencer included in the inventive apparatus, describes a fully **parallel mix columns** transformation. The total number of registers needed for the implementation of the **mix column** transformation in accordance with the preferred embodiment shown in Fig. 7 is 3 wherein two...are
added modulo 2 and loaded into the state register. After the step 709, the **mix columns** transformation is completed and the, state bytes, i.e., the **mix columns** output data can be input in the **add round key** operation 210 in Fig. 2.

1S The inventive apparatus shown in Fig. 1 can also be used for performing an inverse **mix columns** transformation in an efficient manner. As for the **mix columns** transformation, the inverse **mix columns** transformation which is needed for decryption can also be defined to operate on the 16 bytes of the state in **parallel**. The preferred implementation is based on the definition of the Xtime operation given in Figs. 6a and 6b.

For performing the fully **parallel** inverse **mix columns** transformation shown in Fig. 8. the coprocessor needs four temporary registers Tmpl, Tmp2, Tmp3 and...known in the art, a decryption round of the AES algorithm
firstly performs an inverse **shift rows** operation, then an inverse byte substitution operation, then an **add round key** operation and finally an inverse **mix columns** operation.

Therefore, the inverse **mix columns** input data are the data output by the **add round key** operation preceding the inverse

mix columns transformation. Analogously, the content of the state after the step 811 as shown in Fig. 8 is the input in an inverse **shift rows** operation for the next decryption round of the AES algorithm.

Referring to Figs. 9a and 9b, another way to implement the inverse **mix columns** transformation is illustrated. To this end, the two Xtime4 and Xtime8 operations are introduced as... ...m3. Based on the definitions given in Fig. 9, another preferred implementation of the inverse **mix columns** transformation is shown in Fig. 9b.

In a first step 901, a second step 902...811 which have been explained in connection with Fig. 8.

The advantage of the inverse **mix columns** transformation shown in Fig. 9b compared to the implementation shown in Fig. 8 is that the Xtime, Xtime4 and Xtime8 operations can be calculated in **parallel** from the state which avoids the sequence of the first to third steps 801 to ...register, whereupon the twelve rightmost bytes are cleared, i. e., set to zero. The RotWord, **SubByte** and '+ Rcon' operations are preferably done by the main CPU.

In a second step, a...register.

It is to be noted that the RotWord operation and the byte substitution operation (**SubByte**) are performed by the 8-bit CPU ... transformation in the coprocessor is 2. One temporary register is needed for the intermediate resultsf **while** the other temporary register is needed for the key.

The coprocessor is also useful for performing the **add round key** transformation. This transformation is performed by simply adding modulo 2 state and the key inside... ...data registers for holding necessary data for the arithmetic unit of the coprocessor performing a **mix columns** transformation. The arithmetic unit is termed **mix columns** and has the ... stored. The CPU, which is preferably an 8-bit CPU is arranged for performing the **add round key** transformation, the byte substitution operation and the **shift rows** operation. Additionally, in accordance with the embodiment shown in Fig. 12, the CPU is further... ...key expansion and mixed columns can be
performed by the CPU and the coprocessor in **parallel**. This alone can reduce the ...RAM (a very scarce resource) space to the customer's application.

Another advantage when the **mix columns** transformation is performed in the arithmetic unit 1202 of the coprocessor is an improved balance This is due to the fact that the software implementation of the inverse **mix columns** transformation used for decryption is less efficient than the **mix columns** transformation used for encryption. When the inventive apparatus is used for performing the AES algorithm, an improved balance is obtained, since encryption and decryption operations take about the **same time**.

Since the coprocessor performs the multiplication of columns or key words, these operations are protected against timing attacks. Moreover, the **parallel** execution of the **mix columns** and the key expansion transformations makes more difficult power consumption analysis. Additionally, the security can be further enhanced by random masking in the CPU **during** the key expansion and in the coprocessor **during** the **mix columns** operation. The mask is removed **during** the **add round key** transformation. To this end, an additional register in the coprocessor is needed to store a... ...coprocessor includes two calculation units, wherein one calculation unit is used for performing the masking, **while** the other calculation unit in the coprocessor is used for carrying out AES steps.

The main advantages are, however, that the **parallel** implementation of the AES algorithm as outlined above is about two times faster than an implementation in an 8-bit CPU.

Additionally, the **parallel** implementation requires about 3 times less user memory. In fact, an implementation of the AES encryption algorithm on a CPU **together** with a coprocessor having a long integer arithmetic unit requires only 20 bytes of internal...the ALU of the coprocessor is able to perform all operations needed to do the **mix columns** and inverse **mix columns** operations, but it is also possible to perform the AND and RotWord operations in the... ...apparatus
CPU
14 coprocessor
200 sequence of steps
202 AES round
204 Byte Substitution
206 **ShiftRow** Transformation
208 **MixColumns** transformation
210 **AddRoundKey** transformation
300 algorithm input data array
302 State Array

304 algorithm output data array
601 to 606 Steps for calculating Xtime(state)
701 to 709 Steps for Calculating **MixColumns** transformation
801 to 811 Steps for Calculating Inverse **MixColumns** transformation
901 to 911 Steps for Calculating Inverse **MixColumns** transformation
1001 to 1008 Steps for calculating Key Expansion
1100 Step for Calculating **AddRoundKey** transformation
1200 coprocessor register
1202 long arithmetic unit for performing **MixColumns** transformation
1204 CPU memory

Claims:

...for performing a cryptographic algorithm
5 including a sequence of steps, one step including a <B>mix</B> <B>column</B>transformation (208) on <B>mix</B> <B>columns</B> input data to obtain <B>mix</B> <B>columns</B> output data, the <B>mix</B> <B>columns</B> input data having anarray of data groups, the array having a predetermined numberof... ...data group including a number of data units, comprising:a CPU (12) for providing the <B>mix</B> <B>columns</B> input data; anda coprocessor (14) for performing at least a part of the <B>mix</B><B>columns</B> transformation on the <B>mix</B> <B>columns</B> input data, thecoprocessor having an arithmetic unit arranged for conductingcalculations for a number of data units in <B>parallel</B>, thenumber of data units being equal to or greater than the numberof data... ...the AESalgorithm.
3 Apparatus in accordance with claim 1 or 2,
in which the <B>mix</B> <B>columns</B> transformation is defined by amodular multiplication of a matrix derived from a fixedpolynomial by a column of the <B>mix</B> <B>columns</B> input data to obtaina column of the mixed column output data,in which the... ...the matrix by the data groups of one column are performed bythe coprocessor in <B>parallel</B>, wherein a column is interpretedas a polynomial in a finite field having a number... ...claim 3,in which the CPU (12) is arranged to load one column of the <B>mix</B> <B>columns</B> input data to the coprocessor (14) at a time untilall columns of the <B>mix</B> <B>columns</B> input data have been loadedinto the coprocessor, whereinf in response to receiving acolumn of the <B>mix</B> <B>columns</B> input data, the coprocessor (14) isarranged for performing the multiplication in <B>parallel</B> andsumming the results to obtain a data group of the mixedcolumns output dataf andwherein, in response to receiving another column of the <B>mix</B><B>columns</B> input data, the coprocessor (14) is arranged to useanother row of the matrix for...the coprocessor (14) is arranged for performingcalculations on another number of data units in <B>parallel</B>, theother number being greater than or equal to the number of dataunits in the <B>mix</B> <B>columns</B> input data.

7 Apparatus as claimed in claim 6, which is arranged for
performing an operation <B>during</B> the <B>mix</B> <B>columns</B> transformation,the operation being described by multiplying a data group ofthe <B>mix</B> <B>columns</B> input data by two modulo the followingirreducible polynomial:x8+ x4 + X3+ X + 1.

8...having a length equal to or greater than the number of data
units in the <B>mix</B> <B>columns</B> input data and wherein the arithmeticunit is adapted toperform an addition modulo 2...having anorder equal to or greater than the number of data units inthe <B>mix</B> <B>columns</B> input data.

9 Apparatus as claimed in claim 8, wherein the coprocessor is
arranged for...algorithm, and wherein the CPU (12) is arranged to work on the key expansionstep, <B>while</B> the coprocessor works on the <B>mix</B> <B>columns</B> step.

13 Apparatus as claimed in one of claims 1 to 11, in which
another... ...apparatus comprises a key expansion sequencer forcontrolling the following sequence of steps:Tmpl = Rcon + <B>SubByte</B> (RotWord(Key))*Key = Key +TmplTmpl = Tmpl &gt;&gt; 32Key = Key +TmplTmpl = Tmpl &gt;&gt; ...a second temporal register, Rcon is aconstant value, RotWord is a word rotation function, <B>SubByte</B> is a byte substitution function, + is an addition modulo 2, &gt;&gt;is a right shift of...claims 1 to 13,in which another step in the sequence of steps is in <B>add</B> <B>round</B><B>key</B> step wherein the apparatus comprises an <B>add</B> <B>round</B> <B>key</B> sequencer for controlling the following steps:State = Key + state,wherein Key is a contents of...accordance with acryptographic algorithm including a sequence of steps, onestep including an inverse <B>mix</B> <B>columns</B> transformation oninverse <B>mix</B> <B>columns</B> input data to obtain inverse <B>mix</B> <B>columns</B> output data, the inverse <B>mix</B> <B>columns</B> input data having anarray of data groups, the array having a predetermined numberof... ...group including a number of data units, comprising:a CPU (12)for providing the inverse <B>mix</B> <B>columns</B> input data;anda coprocessor (14) for performing at least a part of theinverse <B>mix</B> <B>column</B> transformation on the inverse <B>mix</B> <B>columns</B>input data, the coprocessor having an arithmetic unit arrangedfor conducting calculations for a number of data units in <B>parallel</B>, the number of data units being equal to or greaterthan the number of data... ...algorithm for decryption.

18 Apparatus according to claim 16 or 17, further comprising
an inverse <B>mix</B> <B>columns</B> sequencer for controlling the followingsteps:Tmpl =Xtime(state) ...content.

21 Apparatus as claimed in claim 20, wherein the apparatus
further comprises an inverse <B>mix</B> <B>columns</B> sequencer forcontrolling the following steps:Tmpl = Xtime(state)Tmp2 = Xtime4(state)Tmp3 = Xtime8(state...Method for performing a cryptographic algorithm includinga sequence of steps, one step including a <B>mix</B> <B>column</B>transformation (208) on <B>mix</B> <B>columns</B> input data to obtain <B>mix</B><B>columns</B> output data, the <B>mix</B> <B>columns</B> input data having anarray of data groups, the ...adata group including a number of data units, comprising thefollowing steps:providing the <B>mix</B> <B>columns</B> input data; andperforming at least a

part of the <B>mix</B> <B>columns</B> transformationon the <B>mix</B> <B>columns</B> input data, using an arithmetic unitarranged for conducting calculations for a number of dataunits in <B>parallel</B>, the number of data units being equal to orgreater than the number of data sequence of steps, onestep including an inverse <B>mix</B> <B>columns</B> transformation oninverse <B>mix</B> <B>columns</B> input data to obtain inverse <B>mix</B> <B>columns</B>output data, the inverse <B>mix</B> <B>columns</B> input data having anarray of data groups, the array having a predetermined numberof... ...data group including a number of data units, comprising thefollowing steps:providing the inverse <B>mix</B> <B>columns</B> input data; andperforming at least a part of the inverse <B>mix</B> <B>column</B> transformation on the inverse <B>mix</B> <B>columns</B> input data using anarithmetic unit arranged for conducting calculations for anumber of data units in <B>parallel</B>, the number of data unitsbeing equal to or greater than the number of data...

Dialog eLink: Order File History
9/3K/5 (Item 1 from file: 348)
DIALOG(R)File 348: EUROPEAN PATENTS

01908062

Microprocessor apparatus and method for performing block cipher cryptographic functions
Mikroprozessorvorrichtung und Verfahren zur Durchfuhrung kryptographischer Funktionen zur Blockchiffrierung
Dispositif microprocesseur et procede pour accomplir des fonctions cryptographiques de chiffrage par blocs

Patent Assignee:

- **VIA Technologies, Inc.**; (4548524)
  8F, No.533, Chung-Cheng Rd, Hsin-Tien; Taipei 231,Taiwan; (TW)
  (Proprietor designated states: all)

Inventor:

- **Crispin, Thomas A**
  4005 Lochwood Bend Court; Austin, TX 78738-5015; (US)
- **Henry, Glenn G.**
  411 Lake Cliff Trail; Austin, TX 78746; (US)
- **Parks, Terry**
  6 Carriage House Lane; Austin, TX 78737; (US)

Legal Representative:

- **O'Connell, David Christopher (62553)**
  Haseltine Lake, Redcliff Quay 120 Redcliff Street; Bristol BS1 6HU; (GB)

	Country	Number	Kind	Date	
Patent	EP	1538510	A1	20050608	(Basic)
	EP	1538510	B1	20080813	
Application	EP	2004255590		20040915	
Priorities	US	730167		20031205	

Extended Designated States:
AL; HR; LT; LV; MK;

International Patent Class (V7): G06F-001/00

International Classification (Version 8) IPC	Level	Value	Position	Status	Version	Action	Source	Office
G06F-0001/00	A	I	F	B	20060101	20050124	H	EP

Abstract Word Count: 81
NOTE: 3
NOTE: Figure number on first page: 3

Legal Status Type	Pub. Date	Kind	Text

Language Publication: English
Procedural: English
Application: English

Fulltext Availability Available Text	Language	Update	Word Count
CLAIMS A	(English)	200523	1338
SPEC A	(English)	200523	11539
CLAIMS B	(English)	200833	1452
CLAIMS B	(German)	200833	1321
CLAIMS B	(French)	200833	1609
SPEC B	(English)	200833	11625
Total Word Count (Document A) 12879			
Total Word Count (Document B) 16007			
Total Word Count (All Documents) 28886			

Specification: ...was not many years thereafter before users began to discover the benefits of networking computers **together** to provide shared access to information. Consequently, network architectures, operating systems, and data transmission protocols... ...protect sensitive data and transmissions from unauthorized disclosure has grown dramatically. The number of instances **during** a given computer session where a user is obliged to protect his or her sensitive... ...AES algorithm, the sub-operations within each round are referred to in the literature as **SubBytes** (or **S-box**), **ShiftRows**, MixColums, and **AddRoundKey**. Decryption of a block of ciphertext is similarly accomplished with the exceptions that the ciphertext... ...the input to the inverse cipher and inverse sub-operations are performed (e.g., Inverse **MixColumns**, Inverse **ShiftRows**) **during** each of the rounds, and the final result of the rounds is a block of... ...mode, and output feedback (OFB) mode. Some of these modes utilize an additional initialization vector **during** performance of the sub-operations and some use the ciphertext output of a first set... ...a present day user is confronted with the issue of computer information security many times **during** a work session. For example, under the control of a present day multi-tasking operating system, a user of workstation 101 can be performing several **simultaneous** tasks, each of which require cryptographic operations. The user of workstation 101 is required to... ...the operating system) to store a local file on the network file storage device 106. **Concurrent** with the file storage, the user can transmit an encrypted message to a second user... ...Hence, a computer 101-104 in the near future could potentially be performing hundreds of **concurrent** cryptographic operations.

The present inventors have noted several limitations to the above approach of performing... ...form of add-on boards or external devices that interface to a host processor via **parallel** ports or other interface buses (e.g., USB). These co-processors certainly enable the accomplishment...as supporting interrupts, exceptions, and like events that further exacerbate the problem. Moreover, for every **concurrent** cryptographic operation that is required on a computer system, a separate instance of the applications... ...allocated in memory 203. And, as noted above, it is anticipated that the number of **concurrent** cryptographic operations required to be performed by a microprocessor 201 will continue to increase with... ...other functions within the microprocessor 301. In one embodiment, the cryptography unit 316 operates in **parallel** to other execution units (not shown) within the execution logic 328 such as an integer... ...one embodiment that is compatible with the x86 architecture, the cryptography unit 316 operates in **parallel** with an x86 integer unit, an x86 floating point unit, an x86 MMX(R) unit... ...its expected results are obtained. Alternative x86-compatible embodiments contemplate the cryptography unit operating in **parallel** with a subset of the aforementioned x86 execution units. The cryptography unit 316 is coupled... ...through each of the aforementioned logic stages 302, 303, 304, 307, 314, 316-318 in **synchronization** with a clock signal (not shown) so that operations can be **concurrently** executed in a manner substantially similar to operations performed on an assembly line.

Within the... ...e.g., 0x0FA7), followed a byte detailing a specific block cipher mode to be employed **during** execution of a prescribed cryptographic operation. In one embodiment, the XCRPYT instruction 322 according to ... ...application program to execute on the microprocessor 301. As part of the flow of instructions **during** execution of the application program, an XCRYPT instruction 322 is provided from memory 321 to... ...320 and whose execution is accomplished via a dedicated cryptography unit 316 that operates in **parallel** with and in concert with other execution units within the microprocessor 301. The present inventors... ...of the cryptography unit 316 and associated XCRPYT instruction 322 is entirely compatible with the **concurrent** operation of legacy operating systems 320 and applications, as will be described in more detail... ...The block cipher mode field 404 prescribes the particular block cipher mode to be employed **during** the specified cryptographic operation, as will now be discussed with reference to FIGURE 5.

FIGURE ... ...depicted in FIGURE 6 features execution logic 632 within the execute stage 608 that includes **parallel** execution units 610, 612, 614, 616, 617. An integer unit 610 receives integer micro instructions... ...shares the SSE unit's micro instruction queue 615. An alternative embodiment contemplates stand-alone **parallel** operation of the cryptography unit 617 in a manner like that of units 610, 612... ...are fetched from memory (not shown) by the fetch logic 601 and are provided in **synchronization** with a clock signal (not shown) to the translation logic 602. The translation logic 602 translates each instruction into a corresponding sequence of micro instructions that are sequentially provided in **synchronization** with the clock signal to subsequent stages 605-608, 618, 619 of the microprocessor 600 ...proceed sequentially through the successive stages 605-608, 618, 619 of the microprocessor 600 in **synchronization** with the clock. As micro instructions reach the execute stage 608, they are routed by... ...embodiment, the micro instructions include fields indicating whether or not they can be executed in **parallel** with other operations.

Responsive to fetching an XCRYPT instruction as described above, the translation logic... ...within sequences of cryptography unit micro instructions so that integer operations can be accomplished in **parallel** with cryptography unit operations. Micro instructions are included in the associated micro instructions to allow... ...a second plurality of micro instructions that are executed by one or more of the **parallel** functional units within the microprocessor other that the cryptography unit. The second plurality of micro... ...skilled in the art will appreciate that many cryptographic algorithms perform the same sub-operations **during** each round, except for those performed in the final round. Hence, programming the IRSLT field ... ...schedule that are loaded are placed, in order, in the key RAM 1102 for use **during** their corresponding cryptographic round. Following this, input text data (if an initialization vector is not... ...1211 directs the round engine to employ sub-operations for performing either encryption (e.g., **S**-**Box**) or decryption (e.g., Inverse **S**-**Box**). Contents of bus RNDCON 1212 direct the round engine 1220 to perform either a first... ...coupled to a first register REG-0 1222. The first register 1222 is coupled to **S**-**Box** logic 1223, which is coupled to **Shift Row** logic 1224. The **Shift Row** logic 1224 is coupled to a second register REG-1 1225. The second register 1225 is coupled to **Mix Column** logic 1226, which is coupled to a third register REG-2 1227. The first key logic 1221, **S**-**Box** logic 1223, **Shift Row** logic 1224, and **Mix Column** logic 1226 are configured to perform like-named sub-operations on input text data as is specified in the AES FIPS standard discussed above. The **Mix Columns** logic 1226 is additionally configured to perform AES XOR functions on input data **during** intermediate rounds as required using round keys provided via the key bus 1213. The first key logic 1221, **S**-**Box** logic 1223, **Shift Row** logic 1224, and **Mix Column** logic 1226 are also configured to perform their corresponding inverse AES sub-operations **during** decryption as directed via the state of ENC/DEC 1211. One skilled in the art... ...REG-1 1225 and REG-2 1227. Intermediate round data is pipelined between stages in **synchronization** with a clock signal (not shown). When a cryptographic operation is completed on a block... ...block cryptographic algorithms, the invention also comprehends provision of multiple cryptographic units operatively coupled in **parallel** with other execution units in a conforming microprocessor where each of the multiple cryptographic units...

Specification: ...was not many years thereafter before users began to discover the benefits of networking computers **together** to provide shared access to information. Consequently, network architectures, operating systems, and data transmission protocols... ...protect sensitive data and transmissions from unauthorized disclosure has grown dramatically. The number of instances **during** a given computer session where a user is obliged to protect his or her sensitive... ...AES algorithm, the sub-operations within each round are referred to in the literature as **SubBytes** (or **S-box**), **ShiftRows**, MixColums, and **AddRoundKey**. Decryption of a block of ciphertext is similarly accomplished with the exceptions that the ciphertext... ...the input to the inverse cipher and inverse sub-operations are performed (e.g., Inverse **MixColumns**, Inverse **ShiftRows**) **during** each of the rounds, and the final result of the rounds is a block of... ...mode, and output feedback (OFB) mode. Some of these modes utilize an additional initialization vector **during** performance of the sub-operations and some use the ciphertext output of a first set... ...a present day user is confronted with the issue of computer information security many times **during** a work session. For example, under the control of a present day multi-tasking operating system, a user of workstation 101 can be performing several **simultaneous** tasks, each of which require cryptographic operations. The user of workstation 101 is required to... ...the operating system) to store a local file on the network file storage device 106. **Concurrent** with the file storage, the user can transmit an encrypted message to a second user... ...Hence, a computer 101 -104 in the near future could potentially be performing hundreds of **concurrent** cryptographic operations.

<PATCIT ID=PCIT0001 DNUM=WO03036508A2> WO 03/036508-A2 </PATCIT> teaches a microprocessor... ...form of add-on boards or external devices that interface to a host processor via **parallel** ports or other interface buses (e.g., USB). These co-processors certainly enable the accomplishment...as supporting interrupts, exceptions, and like events that further exacerbate the problem. Moreover, for every **concurrent** cryptographic operation that is required on a computer system, a separate instance of the applications... ...allocated in memory 203. And, as noted above, it is anticipated that the number of **concurrent** cryptographic operations required to be performed by a microprocessor 201 will continue to increase with... ...other functions within the microprocessor 301. In one embodiment, the cryptography unit 316 operates in **parallel** to other execution units (not shown) within the execution logic 328 such as an integer... ...one embodiment that is compatible with the x86 architecture, the cryptography unit 316 operates in **parallel** with an x86 integer unit, an x86 floating point unit, an x86 MMX(R) unit... ...its expected results are obtained. Alternative x86-compatible embodiments contemplate the cryptography unit operating in **parallel** with a subset of the aforementioned x86 execution units. The cryptography unit 316 is coupled... ...through each of the aforementioned logic stages 302, 303, 304, 307, 314, 316-318 in **synchronization** with a clock signal (not shown) so that operations can be **concurrently** executed in a manner substantially similar to operations performed on an assembly line.

Within the... ...e.g., 0x0FA7), followed a byte detailing a specific block cipher mode to be employed **during** execution of a prescribed cryptographic operation. In one embodiment, the XCRPYT instruction 322 according to ... ...application program to execute on the microprocessor 301. As part of the flow of instructions **during** execution of the application program, an XCRYPT instruction 322 is provided from memory 321 to... ...320 and whose execution is accomplished via a dedicated cryptography unit 316 that operates in **parallel** with and in concert with other execution units within the microprocessor 301. The present inventors... ...of the cryptography unit 316 and associated XCRPYT instruction 322 is entirely compatible with the **concurrent** operation of legacy operating systems 320 and applications, as will be described in more detail... ...The block cipher mode field 404 prescribes the particular block cipher mode to be employed **during** the specified cryptographic operation, as will now be discussed with reference to <FIGREF IDREF=F0004... ...F0005>FIGURE 6</FIGREF> features execution logic 632 within the execute stage 608 that includes **parallel** execution units 610, 612, 614, 616, 617. An integer unit 610 receives integer micro instructions... ...shares the SSE unit's micro instruction queue 615. An alternative embodiment contemplates stand-alone **parallel** operation of the cryptography unit 617 in a manner like that of units 610, 612... ...are fetched from memory (not shown) by the fetch logic 601 and are provided in **synchronization** with a clock signal (not shown) to the translation logic 602. The translation logic 602 translates each instruction into a corresponding sequence of micro instructions that are sequentially provided in **synchronization** with the clock signal to subsequent stages 605-608, 618, 619 of the microprocessor 600 ... ...proceed sequentially through the successive stages 605-608, 618, 619 of the microprocessor 600 in **synchronization** with the clock. As micro instructions reach the execute stage 608, they are routed by... ...embodiment, the micro instructions include fields indicating whether or not they can be executed in **parallel** with other operations.

Responsive to fetching an XCRYPT instruction as described above, the translation logic...within sequences of cryptography unit micro instructions so that integer operations can be accomplished in **parallel** with cryptography unit operations. Micro instructions are included in the associated micro instructions to allow... ...a second plurality of micro instructions that are executed by one or more of the **parallel** functional units within the microprocessor other that the cryptography unit. The second plurality of micro... ...skilled in the art will appreciate that many cryptographic algorithms perform the same sub-operations **during** each round, except for those performed in the final round. Hence, programming the IRSLT field ... ...schedule that are loaded are placed, in order, in the key RAM 1102 for use **during** their corresponding cryptographic round. Following this, input text data (if an initialization vector is not... ...1211 directs the round engine to employ sub-operations for performing either encryption (e.g., **S-Box**) or decryption (e.g., Inverse **S-Box**). Contents of bus RNDCON 1212 direct the round engine 1220 to perform either a first... ...coupled to a first register REG-0 1222. The first register 1222 is coupled to **S-Box** logic 1223, which is coupled to **Shift Row** logic 1224. The **Shift Row** logic 1224 is coupled to a second register REG-1 1225. The second register 1225 is coupled to **Mix Column** logic 1226, which is coupled to a third register REG-2 1227. The first key logic 1221, **S-Box** logic 1223, **Shift Row** logic 1224, and **Mix Column** logic 1226 are configured to perform like-named sub-operations on input text data as is specified in the AES FIPS standard discussed above. The **Mix Columns** logic 1226 is additionally configured to perform AES XOR functions on input data **during** intermediate rounds as required using round keys provided via the key bus 1213. The first key logic 1221, **S-Box** logic 1223, **Shift Row** logic 1224, and **Mix Column** logic 1226 are also configured to perform their corresponding inverse AES sub-operations **during** decryption as directed via the state of ENC/DEC 1211. One skilled in the art... ...REG-1 1225 and REG-2 1227. Intermediate round data is pipelined between stages in **synchronization** with a clock signal (not shown). When a cryptographic operation is completed on a block... ...block cryptographic algorithms, the invention also comprehends provision of multiple cryptographic units operatively coupled in **parallel** with other execution units in a conforming microprocessor where each of the multiple cryptographic units...

Claims: ...301, 601), wherein said integer unit (610) and said cryptography unit (316, 617) operate in **parallel** within said microprocessor (201, 301, 601), and wherein said integer operation and said one of the cryptographic operations are accomplished in **parallel**, and wherein said cryptographic instruction (322, 400) explicitly prescribes a block cipher mode (404) to be employed **during** execution of said one of the cryptographic operations, wherein the cryptographic operations comprise:an encryption... ...the cryptographic instruction (322, 400) explicitly prescribes a block cipher mode (404) to be employed **during** execution of the one of the cryptographic operations, and wherein the cryptographic operations comprise:an... ...plaintext blocks; and executing the one of the cryptographic operations and the integer operation in **parallel**, wherein the one of the cryptographic operations is accomplished via a cryptographic unit (316, 617) that is disposed in **parallel** with the integer unit (610) within the processor.

16. The method as recited in claim...

Claims: ...und die Ganzzahleinheit (610) und die Kryptographieeinheit (316, 617) innerhalb des Mikroprozessors (201, 301, 600) **parallel** arbeiten, und die Ganzzahloperation und die eine kryptographische Operation **parallel** ausgefuhrt werden, und der kryptographische Befehl (322, 400) explizit vorschreibt, dass wahrend des Ausfuhrens der... ...eine kryptographische Operation mit Hilfe einer Kryptographieeinheit (316, 317) vorgenommen wird, die innerhalb des Prozessors **parallel** zur Ganzzahleinheit (610) angeordnet ist.

16. Verfahren nach Anspruch 15, wobei das Empfangen umfasst: das...

Dialog eLink: Order File History
9/3K/9 (Item 5 from file: 348)
DIALOG(R)File 348: EUROPEAN PATENTS

01555465

Method for data stream encryption
Verfahren zur Verschlusselung eines Datenstroms
Procede de chiffrage d'un flux de donnees

Patent Assignee:

- **ALCATEL**; (201876)
  54, rue La Boetie; 75008 Paris; (FR)
  (Applicant designated States: all)

Inventor:

- **Cucchi, Silvio**
  Via Gozzadini, 35; 20083 Gaggiano (Milano); (IT)
- **Constantini, Carlo**
  Via Ugo Foscolo,14; 22064 Casatenovo (Lecco); (IT)

Legal Representative:

- **Menzietti, Domenico et al (87745)**
  Alcatel Intellectual Property Department, Via Trento, 30; 20059 Vimercate (Milano); (IT)

	Country	**Number**	**Kind**	**Date**	
Patent	EP	1294124	A2	20030319	(Basic)
	EP	1294124	A3	20031119	
Application	EP	2002292203		20020909	
Priorities	IT	20MI11938		20010917	

Designated States:
AT; BE; BG; CH; CY; CZ; DE; DK; EE; ES;
FI; FR; GB; GR; IE; IT; LI; LU; MC; NL;
PT; SE; SK; TR;

Extended Designated States:
AL; LT; LV; MK; RO; SI;

International Patent Class (V7): H04L-009/06**Abstract Word Count:** 125
NOTE: 2
NOTE: Figure number on first page: 2

Legal Status Type	Pub. Date	Kind	Text

Language Publication: English
Procedural: English
Application: English

Fulltext Availability Available Text	Language	Update	Word Count
CLAIMS A	(English)	200312	525
SPEC A	(English)	200312	2433
Total Word Count (Document A) 2958			
Total Word Count (Document B) 0			
Total Word Count (All Documents) 2958			

Specification: ...to fundamentally repeat, on a regular basis, the following operations on the variable string:

ByteSub; **ShiftRows**; **MixColumn**; **AddRoundKey**.

the **ShiftRows** operation is simply a permutation among the 128 bits;

the **MixColumn** operation is a linear operation, represented - therefore - as a matrix application;

the **AddRoundKey** operation is a module 2 adding operation, (in other words, Xor bit) between the 128...and into a simplified encoder block 22 which applies the simplified Is reversal and a **MixColumn** L operation, in order to generate outgoing transformed bytes w'.

It is to be observed that, **while** describing Figure 1, we have spoken about operations on 8-bit bytes, b, b' and c being vectors of 8 bits, **while** T and M being 8x8 binary matrices.

On the contrary, the coding circuit 21 described... ...as the chaining of 4 bytes, T4 and M4 are block diagonal matrices 32x32, wherein **while** and

Is4 is the simplified reversal operation in the transformed domain operating on 4 bytes independently.

Then, 4 ByteSub operations could be represented as:

As previously made, we neglect the **ShiftRows** operation (it is just a permutation).

As the **MixColumn** operation is a linear operation applied into the encoding block 22, namely a matrix L 32x32, and being the **AddRoundKey** operation the sum of 32 bits of a k4 key through the S2 adder, the... ...a multiplication of the matrix and vector, followed by the sum of the key k4, **while** in the known state of art four reversals (not simplified), a multiplication of the matrix... ...constraint.

According to a further characteristic of the present invention, the encoding circuits 21 operate **jointly** to the schedulers blocks 24, which distribute the computational load on the encoding blocks 22.

Figure 3 describes, therefore, a **parallel** structure encoding system.

The CBC modality, in fact, limits the max. elaboration capacity of a coded circuit, as the encoder circuit 11 or 21.

The **parallel** structure according to Figure 3 forecasts therefore a plurality of encoders blocks 22, for instance... ...is an eighth of the incoming data stream rate Fl, but they contribute, by a **parallel** operation, to reach the desired rate.

An encoder under CBC modalities is not parallelizable per...encoders and therefore of simpler but less expensive type, thanks to the development of a **parallel** architecture.

It is evident that several changes are possible to the manskilled in the art...

Claims: ...Claim 2 characterized by distributing the incoming data stream (Fl) in a plurality (N) of **parallel** data streams (PK) addressed to a plurality of encoding circuits (22) and **parallel** encrypting each one of said data streams (PK).

4. Encryption method of a data stream ...

Dialog eLink: Order File History
14/3K/2 (Item 2 from file: 349)
DIALOG(R)File 349: PCT FULLTEXT

00989343

APPARATUS AND METHOD FOR PERFORMING A CRYPTOGRAPHIC ALGORITHM
APPAREIL ET PROCEDE D'EXECUTION D'UN ALGORITHME CRYPTOGRAPHIQUE

Patent Applicant/Patent Assignee:

- **INFINEON TECHNOLOGIES AG**; St.-Martin-Str. 53, 81669 Munchen
  DE; DE(Residence); DE(Nationality)
  (For all designated states except: US)
- **VALVERDE Antonio**; Unterhachinger Str. 33 a, 81737 Munchen
  DE; DE(Residence); ES(Nationality)
  (Designated only for: US)
- **SEIFERT Jean-Pierre**; Harsdorferstr. 1, 81669 Munchen
  DE; DE(Residence); DE(Nationality)
  (Designated only for: US)

Patent Applicant/Inventor:

- **VALVERDE Antonio**
  Unterhachinger Str. 33 a, 81737 Munchen; DE; DE(Residence); ES(Nationality);
  (Designated only for: US)
- **SEIFERT Jean-Pierre**
  Harsdorferstr. 1, 81669 Munchen; DE; DE(Residence); DE(Nationality);
  (Designated only for: US)

Legal Representative:

- **SCHOPPE Fritz(et al)(agent)**
  Schoppe, Zimmermann, Stockeler & Zinkler, Postfach 71 08 67, 81458 Munchen;
  DE;

	Country	Number	Kind	Date
Patent	WO	200319357	A1	20030306
Application	WO	2001EP9583		20010820
Priorities	WO	2001EP9583		20010820

Designated States: (All protection types applied unless otherwise stated - for applications 2004+)

[EP] AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LU; MC; NL; PT; SE; TR;

[OA] BF; BJ; CF; CG; CI; CM; GA; GN; GQ; GW; ML; MR; NE; SN; TD; TG;

[AP] GH; GM; KE; LS; MW; MZ; SD; SL; SZ; TZ; UG; ZW;

[EA] AM; AZ; BY; KG; KZ; MD; RU; TJ; TM;

Language Publication Language:	English
Filing Language:	English
Fulltext word count:	8257

Detailed Description:

...state
array 302 (Fig. 3) is, therefore, transformed into another state array having a round **key** added. ...into the state. As it is known in the art, a decryption round of the **AES** algorithm firstly performs an inverse **shift rows** operation, then an inverse **byte** substitution operation, then an **add** round **key** operation and finally an inverse mix columns operation.

Therefore, the inverse mix columns input **data** are the **data** output by the **add** round **key** operation preceding the inverse mix columns transformation. Analogously, the content of the state after the...

Dialog eLink: Order File History
14/3K/17 (Item 4 from file: 348)
DIALOG(R)File 348: EUROPEAN PATENTS

01085255

Cryptographic Processing apparatus, cryptographic processing method and storage medium storing cryptographic processing program for realizing high-speed cryptographic processing without impairing security
Vorrichtung und Verfahren zur kryptographischen Verarbeitung sowie Aufzeichnungsmedium zum Aufzeichnen eines kryptographischen Verarbeitungsprogramms zur Ausfuhrung einer schnellen kryptographischen Verarbeitung ohne Preisgabe der Sicherheit
Dispositif et procede de traitement cryptographique ainsi que support d'enregistrement pour stocker un programme de traitement cryptographique afin de realiser un traitement cryptographique rapide sans compromettre la securite

Patent Assignee:

- **MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.**; (1855503)
  1006, Oaza Kadoma; Kadoma-shi, Osaka 571; (JP)
  (Proprietor designated states: all)

Inventor:

- **Ohmori, Motoji**
  1-9-3-402, Nasuzukuri; Hirakata-shi, Osaka-fu 573-0071; (JP)
- **Yokota, Kaoru**
  3-9-202, Shinnozukacho; Ashiya-shi, Hyogo-ken 659-0016; (JP)

Legal Representative:

- **Butcher, Ian James et al (79251)**
  A.A. Thornton & Co. 235 High Holborn; London WC1V 7LE; (GB)

	Country	Number	Kind	Date	
Patent	EP	954135	A2	19991103	(Basic)
	EP	954135	A3	20000607	
	EP	954135	B1	20040407	
Application	EP	99303133		19990422	
Priorities	JP	98116758		19980427	
	JP	98116759		19980427	

Designated States:
DE; FR; GB; IT;

Extended Designated States:
AL; LT; LV; MK; RO; SI;

International Patent Class (V7): H04L-009/06**Abstract Word Count:** 220
NOTE: 7
NOTE: Figure number on first page: 7

Legal Status Type	Pub. Date	Kind	Text

Language Publication:	English
Procedural:	English
Application:	English

Fulltext Availability Available Text	Language	Update	Word Count
CLAIMS A	(English)	199944	5394
SPEC A	(English)	199944	15316
CLAIMS B	(English)	200415	2552
CLAIMS B	(German)	200415	2400
CLAIMS B	(French)	200415	3062
SPEC B	(English)	200415	9840
Total Word Count (Document A) 20714			
Total Word Count (Document B) 17854			
Total Word Count (All Documents) 38568			

Specification: ...An Introduction to Encryption Theory, published by Kyoritsu.

In these cryptosystems, data is divided into **blocks** of 64 **bits** and intensely **shuffled** in units of **blocks**. In the case of the DES algorithm, a **data shuffling** process which combines transposition with substitution is repeated for sixteen stages for each **block**.

One example of the **block ciphers** represented by DES and FEAL is the Blowfish cipher (for details on this cipher, see Bruce Schneier "Description of a New variable-Length **Key**, 64-**Bit Block Cipher** (Blowfish)" in Ross Anderson (ed.) Fast Software Encryption, Lecture Notes in computer Science, vol. 809... ...following is a description of the Blowfish cipher.

Fig. 1 shows the configuration of a **data** encrypting apparatus that uses the Blowfish cipher.

In the figure, a data encrypting apparatus 3010...

Specification: ...An Introduction to Encryption Theory, published by Kyoritsu.

In these cryptosystems, data is divided into **blocks** of 64 **bits** and intensely **shuffled** in units of **blocks**. In the case of the DES algorithm, a **data shuffling** process which combines transposition with substitution is repeated for sixteen stages for each **block**.

One example of the **block ciphers** represented by DES and FEAL is the Blowfish cipher (for details on this cipher, see Bruce Schneier "Description of a New Variable-Length **Key**, 64-**bit Block Cipher** (Blowfish)" in Ross Anderson (ed.) Fast Software Encryption, Lecture Notes in Computer Science, vol 809...

Dialog eLink: Order File History
18/3K/1 (Item 1 from file: 349)
DIALOG(R)File 349: PCT FULLTEXT

01070869

ADVANCED ENCRYPTION STANDARD (AES) HARDWARE CRYPTOGRAPHIC ENGINE
MOTEUR CRYPTOGRAPHIQUE D'EQUIPEMENT TECHNIQUE BASE SUR LA NORME AVANCEE DE CHIFFREMENT (AES)

Patent Applicant/Patent Assignee:

- **ATMEL CORPORATION**; 2325 Orchard Parkway, San Jose, CA 95131
US; US(Residence); US(Nationality)

Legal Representative:

- **SCHNECK Thomas(agent)**
Law Offices of Thomas Schneck, P.O. Box 2-E, San Jose, CA 95109-0005; US;

	Country	Number	Kind	Date
Patent	WO	2003101020	A1	<B>20031204</B>
Application	WO	2003US16326		20030523
Priorities	US	2002383252		20020523

Designated States: (All protection types applied unless otherwise stated - for applications 2004+)

[EP] AT; BE; BG; CH; CY; CZ; DE; DK; EE; ES;
FI; FR; GB; GR; HU; IE; IT; LU; MC; NL;
PT; RO; SE; SI; SK; TR;

[OA] BF; BJ; CF; CG; CI; CM; GA; GN; GQ; GW;
ML; MR; NE; SN; TD; TG;

[AP] GH; GM; KE; LS; MW; MZ; SD; SL; SZ; TZ;
UG; ZM; ZW;

[EA] AM; AZ; BY; KG; KZ; MD; RU; TJ; TM;

Language Publication Language:	English
Filing Language:	English
Fulltext word count:	5808

Detailed Description:

...round constant whenever $i \bmod Nk = 0$. The transformation sequence involves only an S-box **byte substitution** when $Nk > 6$ and $i \bmod Nk = 4$.

The objects of the invention are also met by a pre-**mix** dummy circuit that **inserts** pseudo-random noise into the overall power signature of the hardware **block cipher** circuit during an initial pre-**mix** XOR operation of the **block** cipher algorithm. This differential power analysis countermeasure hides the power signature from all XOR gate...

Inventor search

Dialog eLink: Order File History
35/3/1 (Item 1 from file: 350)
DIALOG(R)File 350: Derwent WPIX

0015945221 *Drawing available*
WPI Acc no: 2006-476887/200649
Fast finite field polynomial divider for ECC and method thereof
Patent Assignee: ELECTRONICS & TELECOM RES INST (ELTE-N)
Inventor: **JUN S I; KIM Y S; LEE S W; LEE Y K; PARK Y S**

Patent Family (2 patents, 1 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	Type
KR 2005065129	A	20050629	KR 200396896	A	20031224	200649	B
KR 564765	B1	20060327	KR 200396896	A	20031224	200724	E

Priority Applications (no., kind, date): KR 200396896 A 20031224

Patent Details

Patent Number	Kind	Lan	Pgs	Draw	Filing Notes	
KR 2005065129	A	KO		1		
KR 564765	B1	KO		1	Previously issued patent	KR 2005065129

Dialog eLink: Order File History
35/3/2 (Item 2 from file: 350)
DIALOG(R)File 350: Derwent WPIX

0015945220 *Drawing available*
WPI Acc no: 2006-476886/200649
Fast finite field polynomial multiplier for ECC(Elliptic Curve Cryptography) and method thereof

Patent Assignee: ELECTRONICS & TELECOM RES INST (ELTE-N)
Inventor: **JUN S I**; **KIM Y S**; **LEE S W**; **LEE Y K**; **PARK Y S**

Patent Family (2 patents, 1 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	Type
KR 2005065128	A	20050629	KR 200396895	A	20031224	200649	B
KR 564764	B1	20060327	KR 200396895	A	20031224	200724	E

Priority Applications (no., kind, date): KR 200396895 A 20031224

Patent Details

Patent Number	Kind	Lan	Pgs	Draw	Filing Notes	
KR 2005065128	A	KO		1		
KR 564764	B1	KO		1	Previously issued patent	KR 2005065128

Dialog eLink: Order File History
35/3/3 (Item 3 from file: 350)
DIALOG(R)File 350: Derwent WPIX

0015867805 *Drawing available*
WPI Acc no: 2006-399481/200641

Method and apparatus for generating prime number for public encryption device, especially related to adding software without additional hardware

Patent Assignee: ELECTRONICS & TELECOM RES INST (ELTE-N)
Inventor: **JUN S I**; **KIM Y S**; **LEE S W**; **LEE Y K**; **PARK Y S**

Patent Family (1 patents, 1 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	Type
KR 2005064107	A	20050629	KR 200395389	A	20031223	200641	B

Priority Applications (no., kind, date): KR 200395389 A 20031223

Patent Details

Patent Number	Kind	Lan	Pgs	Draw	Filing Notes
KR 2005064107	A	KO		1	

Dialog eLink: Order File History
35/3/4 (Item 4 from file: 350)
DIALOG(R)File 350: Derwent WPIX

0015786647 *Drawing available*
WPI Acc no: 2004-673766/200466
Apparatus and method for decrypting block data using rijndael algorithm
Patent Assignee: ELECTRONICS & TELECOM RES INST (ELTE-N); KOREA ELECTRONICS & TELECOM RES INST (KOEL-N)
Inventor: **JUN S I**; **KIM Y S**; **LEE S U**; **LEE Y G**; **PARK Y S**; JEON S I; **LEE S W**

Patent Family (2 patents, 1 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	Type
KR 2004045517	A	20040602	KR 200273321	A	20021123	200466	B
KR 494560	B	20050613	KR 200273321	A	20021123	200659	E

Priority Applications (no., kind, date): KR 200273321 A 20021123

Patent Details

Patent Number	Kind	Lan	Pgs	Draw	Filing Notes	
KR 2004045517	A	KO	1	10		
KR 494560	B	KO			Previously issued patent	KR 2004045517

Dialog eLink: Order File History
35/3/5 (Item 5 from file: 350)
DIALOG(R)File 350: Derwent WPIX

0015786581 *Drawing available*
WPI Acc no: 2004-673696/200466
Modular multiplying device
Patent Assignee: ELECTRONICS & TELECOM RES INST (ELTE-N); KOREA ELECTRONICS & TELECOM RES INST (KOEL-N)

Inventor: JEON S I; JEON Y S; **JUN S I**; JUN Y S; **KIM Y S**; **LEE S U** ; **LEE S W**; **LEE Y G**; **PARK Y S**

Patent Family (2 patents, 1 countries)							
Patent Number	**Kind**	**Date**	**Application Number**	**Kind**	**Date**	**Update**	**Type**
KR 2004045152	A	20040601	KR 200273187	A	20021122	200466	B
KR 481586	B	20050408	KR 200273187	A	20021122	200568	E

Priority Applications (no., kind, date): KR 200273187 A 20021122

Patent Details						
Patent Number	**Kind**	**Lan**	**Pgs**	**Draw**	**Filing Notes**	
KR 2004045152	A	KO	1	10		
KR 481586	B	KO			Previously issued patent	KR 2004045152

Dialog eLink: Order File History
35/3/6 (Item 6 from file: 350)
DIALOG(R)File 350: Derwent WPIX

0015155339 *Drawing available*
WPI Acc no: 2005-504919/200551
XRPX Acc No: N2005-412030
Secure hash algorithms computing apparatus for messaging application, performs logic operation on initial values and input data string stored in register units, and stores value while updating register units
Patent Assignee: CHUNG K (CHUN-I); JUN S I (JUNS-I); KIM Y S (KIMY-I); LEE S W (LEES-I); LEE Y K (LEEY-I); PARK Y S (PARK-I); ELECTRONICS & TELECOM RES INST (ELTE-N)
Inventor: CHUNG K; **JUN S I**; **KIM Y S**; **LEE S W**; **LEE Y K**; **PARK Y S**; CHUNG K I

Patent Family (3 patents, 2 countries)							
Patent Number	**Kind**	**Date**	**Application Number**	**Kind**	**Date**	**Update**	**Type**
US 20050144204	A1	20050630	US 2004917685	A	20040812	200551	B
KR 2005065976	A	20050630	KR 200397149	A	20031226	200641	E
US 7376685	B2	20080520	US 2004917685	A	20040812	200834	E

Priority Applications (no., kind, date): KR 200397149 A 20031226; US 2004917685 A 20040812

Patent Details

Patent Number	Kind	Lan	Pgs	Draw	Filing Notes
US 20050144204	A1	EN	9	4	

Dialog eLink: Order File History
35/3/7 (Item 7 from file: 350)
DIALOG(R)File 350: Derwent WPIX

0014743566 *Drawing available*
WPI Acc no: 2005-091192/200510
XRPX Acc No: N2005-079706
Rijndael block cipher apparatus for cellular phone, encrypts/decrypts 128-bit input data by dividing it into upper 64-bits and lower 64-bits and performing round operation comprising row transformation and round-key addition
Patent Assignee: ELECTRONICS & TELECOM RES INST (ELTE-N); JUN S I (JUNS-I); KIM Y S (KIMY-I); LEE Y K (LEEY-I); PARK Y S (PARK-I); KOREA ELECTRONICS TELECOM (KOEL-N)
Inventor: **JUN S I**; **KIM Y S**; **LEE S U**; **LEE S W**; **LEE Y G**; **LEE Y K**; **PARK Y S**

Patent Family (6 patents, 106 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	Type
WO 2004112309	A1	20041223	WO 2004KR1296	A	20040601	200510	B
KR 2004108311	A	20041223	KR 200364737	A	20030918	200528	E
US 20060147040	A1	20060706	WO 2004KR1296	A	20040601	200645	E
			US 2005560220	A	20051209		
JP 2006527865	W	20061207	WO 2004KR1296	A	20040601	200682	E
			JP 2006516910	A	20040601		
CN 1833399	A	20060913	CN 200480022446	A	20040601	200706	E
KR 710455	B1	20070424	KR 200364737	A	20030918	200832	E

Priority Applications (no., kind, date): KR 200338892 A 20030616; KR 200364737 A 20030918

Patent Details

Patent Number	**Kind**	**Lan**	**Pgs**	**Draw**	**Filing Notes**	
WO 2004112309	A1	EN	58	8		
National Designated States,Original	AE AG AL AM AT AU AZ BA BB BG BR BW BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE EG ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NA NI NO NZ OM PG PH PL PT RO RU SC SD SE SG SK SL SY TJ TM TN TR TT TZ UA UG US UZ VC VN YU ZA ZM ZW					
Regional Designated States,Original	AT BE BG BW CH CY CZ DE DK EA EE ES FI FR GB GH GM GR HU IE IT KE LS LU MC MW MZ NA NL OA PL PT RO SD SE SI SK SL SZ TR TZ UG ZM ZW					
US 20060147040	A1	EN			PCT Application	WO 2004KR1296
JP 2006527865	W	JA	40		PCT Application	WO 2004KR1296
					Based on OPI patent	WO 2004112309
KR 710455	B1	KO			Previously issued patent	KR 2004108311

Dialog eLink: Order File History
35/3/8 (Item 8 from file: 350)
DIALOG(R)File 350: Derwent WPIX

0014543013 *Drawing available*
WPI Acc no: 2004-724967/200471
Polynomial multiplication device for block encryption and multiplying method
Patent Assignee: ELECTRONICS & TELECOM RES INST (ELTE-N); KOREA ELECTRONICS & TELECOM RES INST (KOEL-N)
Inventor: **JUN S I**; **KIM Y S**; **LEE S U**; **LEE Y G**; **PARK Y S**; JEON S I; **LEE S W**

Patent Family (2 patents, 1 countries)

Patent Number	**Kind**	**Date**	**Application Number**	**Kind**	**Date**	**Update**	**Type**
KR 2004047105	A	20040605	KR 200275193	A	20021129	200471	B
KR 498736	B	20050701	KR 200275193	A	20021129	200660	E

Priority Applications (no., kind, date): KR 200275193 A 20021129

Patent Details

Patent Number	Kind	Lan	Pgs	Draw	Filing Notes	
KR 2004047105	A	KO	1	10		
KR 498736	B	KO			Previously issued patent	KR 2004047105

Dialog eLink: Order File History
24/3/1 (Item 1 from file: 349)
DIALOG(R)File 349: PCT FULLTEXT

01189507

RIJNDAEL BLOCK CIPHER APPARATUS AND ENCRYPTION/DECRYPTION METHOD THEREOF
APPAREIL DE CHIFFREMENT PAR BLOC DE RIJNDAEL ET PROCEDE DE CHIFFREMENT/DECHIFFREMENT CORRESPONDANT

Patent Applicant/Patent Assignee:

- **ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUE**; 161 Gajeong-Dong, Yuseong-Gu, Daejon 305-350
  KR; KR(Residence); KR(Nationality)
  (For all designated states except: US)
- **LEE Yun Kyung; 153-1 Munoe-dong, Yeongcheon, Kyungsangbook-Do 770-030
  KR; KR(Residence); KR(Nationality)
  (Designated only for: US)**
- **PARK Young Soo; 101-907 SanHo APT., Tanbang-dong, Seo-Gu, Daejon 101-907
  KR; KR(Residence); KR(Nationality)
  (Designated only for: US)**
- **KIM Young Sae; 202-101 YuseongMokryun Apt., Sangdai-Dong, Yuseong-Gu, Daejon 305-313
  KR; KR(Residence); KR(Nationality)
  (Designated only for: US)**
- **LEE Sang Woo; 218-201 Mannyeon-Dong, Seo-Gu, Daejon 302-150
  KR; KR(Residence); KR(Nationality)
  (Designated only for: US)**
- **JUN Sung Ik; 107-704 Hanbit APT., Eoeun-Dong, Yuseong-Gu, Daejon 305-333
  KR; KR(Residence); KR(Nationality)
  (Designated only for: US)**

Patent Applicant/Inventor:

- **LEE Yun Kyung
  153-1 Munoe-dong, Yeongcheon, Kyungsangbook-Do 770-030; KR; KR(Residence); KR(Nationality); (Designated only for: US)**
- **PARK Young Soo
  101-907 SanHo APT., Tanbang-dong, Seo-Gu, Daejon 101-907; KR; KR(Residence); KR(Nationality); (Designated only for: US)**

- **KIM Young Sae**
  202-101 YuseongMokryun Apt., Sangdai-Dong, Yuseong-Gu, Daejon 305-313; KR; KR(Residence); KR(Nationality); (Designated only for: US)
- **LEE Sang Woo**
  218-201 Mannyeon-Dong, Seo-Gu, Daejon 302-150; KR; KR(Residence); KR(Nationality); (Designated only for: US)
- **JUN Sung Ik**
  107-704 Hanbit APT., Eoeun-Dong, Yuseong-Gu, Daejon 305-333; KR; KR(Residence); KR(Nationality); (Designated only for: US)

Legal Representative:

- **LEE Hwa Ik(agent)**
  YOUNG INTERNATIONAL PATENT& LAW FIRM, 4th Fl. Yosam Bldg. 648-23, Yoksam-Dong, Kangnam-Gu, Seoul 135-748; KR;

	Country	Number	Kind	Date
Patent	WO	2004112309	A1	20041223
Application	WO	2004KR1296		20040601
Priorities	KR	1020030038892		20030616
	KR	1020030064737		20030918

Designated States: (All protection types applied unless otherwise stated - for applications 2004+)
AE; AG; AL; AM; AT; AU; AZ; BA; BB; BG;
BR; BW; BY; BZ; CA; CH; CN; CO; CR; CU;
CZ; DE; DK; DM; DZ; EC; EE; EG; ES; FI;
GB; GD; GE; GH; GM; HR; HU; ID; IL; IN;
IS; JP; KE; KG; KP; KZ; LC; LK; LR; LS;
LT; LU; LV; MA; MD; MG; MK; MN; MW; MX;
MZ; NA; NI; NO; NZ; OM; PG; PH; PL; PT;
RO; RU; SC; SD; SE; SG; SK; SL; SY; TJ;
TM; TN; TR; TT; TZ; UA; UG; US; UZ; VC;
VN; YU; ZA; ZM; ZW;

[EP] AT; BE; BG; CH; CY; CZ; DE; DK; EE; ES;
FI; FR; GB; GR; HU; IE; IT; LU; MC; NL;
PL; PT; RO; SE; SI; SK; TR;

[OA] BF; BJ; CF; CG; CI; CM; GA; GN; GQ; GW;
ML; MR; NE; SN; TD; TG;

[AP] BW; GH; GM; KE; LS; MW; MZ; NA; SD; SL;
SZ; TZ; UG; ZM; ZW;

[EA] AM; AZ; BY; KG; KZ; MD; RU; TJ; TM;

Language Publication Language:	English
Filing Language:	English
Fulltext word count:	23015